REMARKS/ARGUMENTS

In this Amendment Under 37 C.F.R. § 1.111 ("Amendment"), Applicants cancel, without prejudice or disclaimer, claim 1; amend independent claims 2, 12, 16, and 17 to recite, inter alia, "of a computer system, communication network, or computer system and communication network that uses a public-key cryptographic algorithm"; amend claim 15 to recite, inter alia, "a multiplexer adapted to receive inputs -2A, -A, 0, A, 2A" and "adapted to select one of the inputs -2A, -A, 0, A, 2A based on the third selection signal in an integer modular multiplication mode"; amend claim 16 to recite, inter alia, "for receiving an n-bit modulus M, a previous sum, a current partial product, and a multiplicand" and "adapted to receive the n-bit modulus M, the previous sum, the current partial product, and the multiplicand"; and amend claim 17 to recite, inter alia, "adapted to receive first inputs -2A, -A, 0, A, 2A" and "adapted to select one of the first inputs -2A, -A, 0, A, 2A"; all in order to better define the claimed invention. Applicants also make other amendments to claims 2-17 in order to improve clarity. No new matter is introduced.

Prior to entry of the Amendment, claims 1-17 were pending in the application. After entry of the Amendment, claims 2-17 are pending in the application.

In the Office Action, the Examiner rejected claims 15-17 under 35 U.S.C. § 112, ¶ 2; alleged that claim 1 conflicted with claim 61 of U.S. Application No. 10/736,832 ("the '832 application"); provisionally rejected claim 1 under

35 U.S.C. § 101 over claim 61 of the '832 application; provisionally rejected claim 1 on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 51-60 of the '832 application; rejected claims 1-17 under 35 U.S.C. § 101; rejected claim 16 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,206,827 to Tsuruta ("Tsuruta"); and rejected claim 1 under 35 U.S.C. § 103(a) as being unpatentable over "New VLSI Architecture of RSA Public-Key Cryptosystem" by Wang et al. ("Wang").

Applicants respectfully traverse the Examiner's rejection under 35 U.S.C. § 102(b).

Claim Rejection Under 35 U.S.C. § 112, ¶ 2

As discussed above, Applicants amend claim 15 to recite, inter alia, "a multiplexer adapted to receive inputs -2A, -A, 0, A, 2A" and "adapted to select one of the inputs -2A, -A, 0, A, 2A based on the third selection signal in an integer modular multiplication mode"; amend claim 16 to recite, inter alia, "for receiving an n-bit modulus M, a previous sum, a current partial product, and a multiplicand" and "adapted to receive the n-bit modulus M, the previous sum, the current partial product, and the multiplicand"; and amend claim 17 to recite, inter alia, "adapted to receive first inputs -2A, -A, 0, A, 2A" and "adapted to select one of the first inputs -2A, -A, 0, A, 2A".

Applicants submit that these amendments obviate the Examiner's rejection under 35 U.S.C. § 112, ¶ 2.

Claim 1

As discussed above, Applicants cancel, without prejudice or disclaimer, claim 1. Applicants submit that this cancellation resolves all potential issues associated with claim 1 of the present application.

Claim Rejection Under 35 U.S.C. § 101

As discussed above, Applicants amend independent claims 2, 12, 16, and 17 to recite, inter alia, "of a computer system, communication network, or computer system and communication network that uses a public-key cryptographic algorithm".

Applicants submit that claims 2, 12, 16, and 17, at least as amended, accomplish a practical application; that the practical application yields a real-world result that is useful, tangible, and concrete; and that none of claims 2, 12, 16, and 17 covers every substantial practical application. As a result, Applicants submit that these amendments obviate the Examiner's rejection under 35 U.S.C. § 101.

Claim Rejection Under 35 U.S.C. § 102(b)

Applicants submit that the Examiner has failed to establish a proper prima facie case of anticipation for at least the following reasons.

In FIG. 3 of Tsuruta, the output of partial remainder quadruple generation circuit 16 is a quadruple of a partial remainder R(j) sent from the subsequent partial remainder generation circuit 17, not a previous sum; the output of subsequent partial remainder generation circuit 17 is a partial

remainder, not a current partial product; and $R^{(0)}$ is a dividend, not a multiplicand. Tsuruta, c. 3/ll. 37-51 and FIG. 3.

For at least these reasons, Applicants submit that independent claim 16 is patentable under 35 U.S.C. § 102(b) over Tsuruta.

Request for Reconsideration and Allowance

Accordingly, in view of the above amendments and remarks, reconsideration of the rejections and allowance of each of claims 2-17 in connection with the present application is earnestly solicited.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

If necessary, the Director of the U.S. Patent and Trademark Office is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; in particular, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By _____

John A. Castellano, Reg. No. 35,094

P.O. Box 8910
Reston, VA 20195
703.668.8000

JAC/LFG/krm